Snyk と The Linux Foundation による共同調査

オープンソースソフトウェアにおける セキュリティの現状に関するレポート

オープンソースにおける脆弱性の修正にかかる時間は 2018 年から約 2 倍以上増加

デベロッパーファーストのセキュリティプラットフォームを提供する Snyk 株式会社（本社：東京都渋谷区、代表：秋山将人）は、The Linux Foundation との共同調査を実施し、「オープンソースソフトウェアにおけるセキュリティの現状（The State of Open Source Security）」レポートを本日公開しました。

本レポートでは、最新のアプリケーション開発においてオープンソースソフトウェアが広く使用されていることから生じる重大なセキュリティリスクと、これらのリスクを効果的に管理するための準備が多くの企業や組織で整っていない事実が明らかになりました。

主な調査結果

- 41%の企業がオープンソースソフトウェアのセキュリティを信頼していない

- アプリケーション開発プロジェクトには平均で 49 件の脆弱性があり、80 件の直接依存関係があることが判明
- オープンソースプロジェクトにおける脆弱性の修正にかかる時間は確実に増加する一方で、2018 年に 49 日だったものから 2021 年には 110 日と 2 倍以上に増加

Snyk デベロッパーリレーションズ、ディレクター、マット・ジャーヴィス氏のコメント

「現在のソフトウェア開発者は、独自のサプライチェーンを持っています。大きな部分を組み立てる代わりに、既存のオープンソースコンポーネントに独自のコードをパッチングしてコードを組み立てているのです。これは生産性の向上とイノベーションにつながりますが、同時にセキュリティ上の大きな懸念も生じています。このレポートでは、現在のオープンソースセキュリティの状況について、業界の甘さを示唆する証拠が広く発見されました。私たちは、The Linux Foundation とともに、この調査結果を活用して、世界中の開発者をさらに教育し、安全性を維持しながら高速なビルドを継続できるよう支援します」

Open Source Security Foundation (OpenSSF)、General Manager、Brian Behlendorf 氏のコメント

「オープンソースソフトウェアは、開発者の効率を高め、イノベーションを加速させることは間違いありませんが、最新のアプリケーションを組み立てる方法は、セキュリティを確保することをより困難なものにしています。このレポートは、セキュリティリスクが現実であることを明確に示しています。一般的なオープンソースコンポーネントに脆弱性が発見され、組織が直接影響を受けるかどうか、どのように対応すべきかを把握するために奔走するという、あまりにもありふれたシナリオを回避するために、業界全体で協力する必要があるのです」

41%の組織がオープンソースソフトウェアのセキュリティを信頼していない

現代のアプリケーション開発チームは、あらゆるところからコードを活用しています。彼らは、自分たちが構築した他のアプリケーションのコードを再利用し、コードリポジトリを検索して、必要な機能を提供するオープンソースのコンポーネントを見つけます。オープンソースの利用には、開発者のセキュリティについて新しい考え方が必要ですが、多くの企業や組織ではまだ採用されていません。

また、本レポートにより、オープンソースソフトウェアの開発または使用に関するセキュリティポリシーを策定している企業や組織は 49%、中堅から大手企業ではわずか 27%しか策定されていませんでした。
さらに、オープンソースセキュリティポリシーを持たない企業や組織の 30%は、チーム内でオープンソースセキュリティに直接取り組んでいる人材がいないことを認めています。

平均的なアプリケーション開発プロジェクトに 80 の直接的な依存関係にまたがる 49 の脆弱性

オープンソースのコンポーネントをアプリケーションに組み込むと、開発者は即座にそのコンポーネントに依存することになり、そのコンポーネントに脆弱性が含まれていた場合、危険にさらされることになります。本レポートは、このリスクがいかに現実的であるかを示しており、評価した各アプリケーションの多くの直接的な依存関係において、数十の脆弱性が発見されています。
このようなリスクは、間接的な依存関係、つまり依存する依存関係によってさらに深刻化します。多くの開発者はこのような依存関係を知らないため、追跡とセキュリティ確保がより困難になっています。
しかし、本調査の回答者は、現在のソフトウェアサプライチェーンにおいて、オープンソースが生み出すセキュリティの複雑さをある程度認識しているようです：

- 調査回答者の 4 分の 1 以上が、直接依存関係におけるセキュリティの影響を懸念していると回答
- 推移的な依存関係に対して実施しているコントロールに自信があると答えた回答者は、わずか 18%
- 全脆弱性の 40%は、推移的な依存関係において発見された

脆弱性の修正にかかる時間が 2018 年の 49 日から 2021 年は 110 日と 2 倍以上に増加

アプリケーション開発が複雑化するにつれて、開発チームが直面するセキュリティ上の課題も複雑化しています。開発を効率化する一方で、オープンソースソフトウェアの使用は、修正の負担を増大させます。本レポートによると、オープンソースプロジェクトにおける脆弱性の修

正には、プロプライエタリ（私有）なプロジェクトに比べて 20%近く（18.75%）の時間がかかることが明らかになりました。

本レポートについて

オープンソースソフトウェアにおけるセキュリティの現状（The State of Open Source Security）レポートは、Snyk と The Linux Foundation によるパートナーシップで、OpenSSF、Cloud Native Security Foundation、Continuous Delivery Foundation、Eclipse Foundation がサポートしています。2022 年第 1 四半期に行われた 550 人以上の回答者への調査と、13 億以上のオープンソースプロジェクトを分析してきた Snyk Open Source のデータに基づいています。

Snyk について

Snyk はデベロッパーファーストのセキュリティプラットフォームです。コードやオープンソースとその依存関係、コンテナや IaC(Infrastructure as Code) における脆弱性を見つけるだけでなく、優先順位をつけて修正するためのツールです。Git や統合開発環境（IDE）、CI/CD パイプラインに直接組み込むことができるので、開発者が簡単に使うことができます。

Snyk は現在、Asurion、Google、Intuit、MongoDB、New Relic、Revolut、Salesforce などの業界リーダーを含む、世界中の 1,500 社以上の顧客に利用されています。

Snyk は、Forbes Cloud 100 2021、2021 CNBC Disruptor 50、2021 Gartner Magic Quadrant for AST で Visionary に選ばれています。

ウェブサイト: https://snyk.io/jp

資料請求：https://go.snyk.io/jp-shiryoseikyu.html

The Linux Foundation について

The Linux Foundation は、オープン テクノロジーの開発と商業的普及を加速するエコシステムを構築するために、世界のトップ開発者や企業から選ばれている組織です。世界中のオープンソース コミュニティとともに、歴史上最大の共有技術投資を実現することで、最も困難な技術的問題を解決しています。2000 年に設立された The Linux Foundation は、今日、あらゆるオープン ソース プロジェクトを拡張するためのツール、トレーニング、イベントを提供してお

り、これらを組み合わせることで、一企業では達成できない経済効果を実現しています。詳細については、www.linuxfoundation.org をご覧ください。

【報道関係者連絡先】

Snyk 株式会社

担当：中野

Email: info-japan@snyk.io
Tel: 03-6822-0629

Snyk 広報事務局

担当：伊藤、大木、ジェレミー

Email: contact@kartz.co.jp
Tel: 03-6427-1627